

## BUNDESREPUBLIK DEUTSCHLAND

REC'D 20 OCT 2000

WIPO PCT

PRIORITY  
DOCUMENTSUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)EPO - Munich  
12

02. Okt. 2000

EP 00/08516

Prioritätsbescheinigung über die Einreichung  
einer Patentanmeldung 4

Aktenzeichen:

199 41 868.3

Anmeldetag:

02. September 1999

Anmelder/Inhaber:

GZS Gesellschaft für Zahlungssysteme mbH,  
Bad Vilbel/DE; INFORM GmbH, Aachen/DE.

Bezeichnung:

Expertensystem

IPC:

G 06 F, G 07 F

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 21. September 2000  
Deutsches Patent- und Markenamt  
Der Präsident  
Im Auftrag

Nietiert

Patentanwälte

Dr. Walter Maiwald (München)  
Dr. Volker Hamm (Hamburg)  
Dr. Stefan Michalski (München)  
Dr. Regina Neuefeind (München)

Rechtsanwalt

Stephan N. Schneller (München)

In Kooperation mit:

Dr. Schmidt-Felzmann & Koziarka  
Rechtsanwälte  
(Hamburg)

Parr · Tauche · Jaeger ·  
Leutheusser - Schnarrenberger  
Rechtsanwälte  
(München · Starnberg)

Aktenzeichen  
Neuanmeldung

Unser Zeichen  
G 7166 / WM

GZS Gesellschaft für Zahlungssysteme mbH  
INFORM GmbH

München,  
1. September 1999

GZS Gesellschaft für Zahlungssysteme mbH,  
60298 Frankfurt;  
INFORM GmbH,  
Pascalstraße 23, 52076 Aachen

-----  
Expertensystem  
-----

Die Erfindung betrifft den Nachweis der betrügerischen Verwendung von Kundenkonten und Kontonummern, einschließlich von zum Beispiel Geschäften mit Kreditkarten. Insbesondere betrifft die Erfindung ein automatisiertes Betrugsnachweissystem und ein Verfahren, das ein Vorhersagemodell zur Mustererkennung und Klassifizierung verwendet, um Geschäfte mit einer hohen Betrugswahrscheinlichkeit auszusondern.

In der folgenden Diskussion wird der Ausdruck "Kreditkarte" zu Zwecken der Anschaulichkeit verwendet; jedoch gelten die hier diskutierten Methoden und Grundlagen auch für andere Arten von elektronischen Zahlungssystemen, wie etwa Kundenkreditkarten, automatisierte maschinenlesbare Kassenkarten und Telefonkarten.

Seit jeher haben die Emittenden von Kreditkarten versucht, ihre Verluste durch Betrug zu begrenzen, indem die betrügerische Verwendung der Karte aufgezeigt wird, bevor der Karteninhaber eine verlorene oder gestohlene Karte gemeldet hat.

Ein wirksames Modell zum Betrugsnachweis sollte hohe Fangraten bei niedriger Verhinderung rechtmäßiger Transaktionen im Echtzeitbetrieb ergeben. Es sollte sich verändernden Betrugsmethoden und -muster anpassen können, und sollte eine integrierte Lernfähigkeit aufweisen, welche diese Anpassungsfähigkeit unterstützt.

Die vorveröffentlichte Druckschrift WO-A-8 906 398 beschreibt ein Element zur Analyse einer Transaktion mittels Datenverarbeitung: indem nur diejenigen Daten herausgezogen werden, die zur Analyse der Transaktion nützlich sind; Signale gelöscht werden, die einer Transaktion entsprechen, von der man meint, daß sie auf einen Satz vorbestimmter Regeln paßt; gefiltert wird, damit nicht-signifikante Abwandlungen der zu analysierenden Transaktion beseitigt werden; und die Signale in eine oder mehrere Klassen, gemäß einem vorbestimmten Kriterium, eingeteilt werden. Dieses Element ist zur Anwendung für die Herausgabe von Zahlungsautorisierungen an Kreditkartennutzer geeignet.

Eine weitere Druckschrift, EP-A-0 418 144 beschreibt ein Verfahren zur Begrenzung der mit einer computergestützten Transaktion verbundenen Risiken, indem die Transaktionsanfrage mit vorbestimmten statistischen Daten verglichen wird, die als repräsentativ zur Risikobewertung einer nicht gemäßen Verwendung erscheinen. Die statistischen Daten beschreiben die gemittelte Anzahl oder die Menge der während der Abfolge von aufeinanderfolgenden Zeitabschnitten getätigten Transaktionen, und werden

abgeleitet, indem die Zeit in aufeinanderfolgende nicht gleiche Abschnitte eingeteilt wird, deren Dauern so gewählt sind, daß die Wahrscheinlichkeit einer getätigten Transaktion oder der gemittelte Betrag für jeden einzelnen Zeitabschnitt im wesentlichen gleich sind.

Aus der EP-0 669 032 sind ein auf einem Computer implementiertes Betrugsnachweisverfahren und eine entsprechende Hardware bekannt, welche Einrichtungen für Vorhersagemodelle einschließt. Aktuelle Transaktionsdaten werden empfangen und verarbeitet, was dann in einer Vielzahl von Ausgabewerten resultiert, die einen Trefferwert enthalten, der die Wahrscheinlichkeit für eine betrügerische Transaktion darstellt.

Dieses im Stand der Technik bekannte Verfahren erfordert mehrere Schritte, die vor den Verarbeitungsschritten für die aktuellen Daten durchgeführt werden müssen, nämlich:

- Erzeugen eines Benutzerprofils für jeden einzelnen einer Vielzahl von Benutzern aus einer Unmenge von Variablen bezüglich früheren Transaktionen und aus persönlichen Benutzerdaten, die für jeden Benutzer Werte aus einer Vielzahl von Benutzervariablen enthalten, wobei jedes Benutzerprofil ein Muster für die Tätigkeitshistorie eines Benutzers beschreibt;
- Ableitung von Variablen, die nachgewiesenen früheren Betrug betreffen, indem Daten früherer Transaktionen vorverarbeitet werden, wobei diese Werte für eine Vielzahl von Transaktionsvariablen für eine Vielzahl von früheren Transaktionen beinhalten;
- Trainieren von Einrichtungen für Vorhersagemodelle mit den Benutzerprofilen und mit den Variablen, die früheren Betrug betreffen, um ein Vorhersagemodell zu erhalten; und

- Speichern des erhaltenen Vorhersagemodells im Computer.

Dann erfolgt die Verarbeitung der aktuellen Daten, indem

- die aktuellen Transaktionsdaten für eine aktuelle Transaktion eines Benutzers empfangen werden;
- die Benutzerdaten, die den Benutzer betreffen, empfangen werden;
- das mit dem Benutzer verbundene Benutzerprofil empfangen wird;
- die erhaltenen aktuellen Transaktionsdaten, Benutzerdaten und Benutzerprofil vorverarbeitet werden, um für die aktuelle Transaktion Variablen bezüglich eines aktuellen Betruges abzuleiten;
- die Betrugswahrscheinlichkeit bei der aktuellen Transaktion bestimmt wird, indem das Vorhersagemodell auf die aktuellen betrugsbezogenen Variablen angewendet wird; und
- von den Einrichtungen für das Vorhersagemodell ein Ausgangssignal abgegeben wird, welches die Betrugswahrscheinlichkeit für die aktuelle Transaktion anzeigt.

Dieses System stützt sich auf ein neuronales Netz, um die Einrichtungen für das Vorhersagemodell zu trainieren. Dieses Training soll hauptsächlich die Einrichtungen für das Vorhersagemodell verändern, um die Verhinderung rechtmäßiger Transaktionen gering zu halten und die Leistung des Systems für den Betrugsnachweis zu verbessern.

Hierbei stützt sich das System auf einen Satz von festen (aber veränderbaren) Werten, die verschiedene Aspekte der Transaktion darstellen. Diese Werte werden in der Verarbeitung

unterschiedlich gewichtet und eine wichtige Funktion des auf dem neuronalen Netz basierenden Trainings ist die Veränderung dieser Gewichtung, was in grundlegender Weise eine "Lern"-Fähigkeit für dieses System ergibt. Solche bekannten neuronalen Netze stellen eine Verknüpfung von „Neuronen“ im Sinne einfacher mathematischer Übertragungsfunktionen dar. Um hier eine „Lernfähigkeit“ zu erzeugen, wird ein entsprechender Algorithmus eingesetzt - z.B. gemäß EP 0 669 032 zur Anpassung der „Gewichte“ bei der Datenbewertung im neuronalen Netz.

Bei alledem verwendet das System für die Kombination der verschiedenen Parameter und Daten gewöhnliche Logikalgorithmen und funktionelle Beziehungen, um den Trefferwert zu erhalten. Es führt für jede aktuelle Transaktion eine Berechnung durch, die auf herkömmlicher Logik basiert, betrachtet (später) das Ergebnis und verändert, wenn notwendig, den Algorithmus.

Es ist wünschenswert, ein automatisiertes System zu schaffen, welches die verfügbaren Informationen z.B. über den Karteninhaber, Händler und Geschäfte verwendet, um Transaktionen zu prüfen und jene auszusondern, die wahrscheinlich betrügerisch sind, und dabei einen relativ höheren Anteil an Betrugsfällen bei einer relativ niedrigen Verhinderung rechtmäßiger Transaktionen auffinden kann. Ein solches System sollte vorzugsweise noch fähig sein, mit einer großen Zahl von voneinander abhängigen Variablen in einem schnellen Echtzeitbetrieb umzugehen, und sollte die Fähigkeit zur Rückentwicklung des zugrundeliegenden Systemmodells als neue Muster für auftauchendes Betrugsverhalten aufweisen.

Demgemäß betrifft die Erfindung ein in einem Computer implementiertes Verfahren zur Identifizierung und Bestimmung von betrügerischen Transaktionsdaten, gemäß den Merkmalen des Anspruchs 1.

In mancher Hinsicht verwendet die Erfindung Merkmale, die aus der EP 0 669 032 bekannt sind. Auf die EP 0 669 032 wird deshalb in vollem Umfang Bezug genommen.

Jedoch gibt es, wie aus der folgenden Beschreibung erkennbar, größere Unterschiede zwischen der Erfindung und diesem Stand der Technik, die sowohl in der grundlegenden Herangehensweise und der entsprechenden Grundstruktur, als auch in verschiedenen Einzelheiten der Datenerzeugung und -verarbeitung liegen.

Ein wesentlicher Unterschied ergibt sich daraus, daß die vorliegende Erfindung kein Benutzerprofil als Teil des Vorhersagemodells verwendet. Statt dessen arbeitet die Erfindung mit einer Kombination von einerseits Expertenregeln und andererseits einer Analyse vorausgegangener Benutzungsvorgänge des Zahlungsmittels, das für die aktuell zu bewertende Transaktion eingesetzt wird.


Bei den Expertenregeln handelt es sich, vergleichbar dem eingangs genannten Stand der Technik, um eine auf Erfahrungswerten, i.e. der Analyse früherer Mißbrauchsfälle, basierende Auswahl typischer Elemente einer individuellen Transaktion, die eine erhöhte Gefahr eines Mißbrauchs anzeigen. Relevant sind erfindungsgemäß insbesondere die Herkunft des Zahlungsmittels (zum Beispiel der Karte), die Branche und die Person des Empfängers der zu autorisierenden Zahlung und der Betrag der Zahlung.

Die Analyse vorausgegangener Benutzungsvorgänge desselben Zahlungsmittels umfaßt vorzugsweise die jüngsten Vorgänge, etwa die letzten fünf bis zwanzig Transaktionen (könnte sich aber auch weiter zurück erstrecken).

Im Gegensatz zum Stand der Technik, zum Beispiel gemäß EP 0 669 032, verwendet die Erfindung vorzugsweise kein herkömmliches neuronales Netz, kombiniert mit einem Lernalgorithmus.

Die Erfindung verwendet Fuzzy Logik zur Feststellung, ob eine bestimmte Transaktion als betrügerisch zu erachten ist.

Im erfindungsgemäß bevorzugten Entscheidungssystem werden sowohl die Expertenregeln als auch dem neuronalen Netz im Stand der Technik funktional entsprechenden Regeln für die deskriptive Statistik als Fuzzy-Regeln abgespeichert, und unterscheiden sich damit nicht in der Berechnungsart, jedoch in der Gewinnungsart.



Das Expertenwissen ist direkt als Fuzzy-Regeln formuliert. Diese definieren für jede Transaktionsart ein Limit, das der (benutzerspezifischen) „Risikobereitschaft“ entspricht.

Die Information aus der Benutzungshistorie des Zahlungsmittels wird mit Hilfe eines „NeuroFuzzy-Moduls“ ebenfalls in Fuzzy-Regeln transformiert. Das NeuroFuzzy Modul verwendet eine Modifikation desjenigen Trainingsalgorithmus, der auch bei den meisten neuronalen Netzen verwendet wird, nämlich den Error Backpropagation Algorithmus, der weithin in der Literatur beschrieben ist. Da in dieser Weise die Information aus den Vergangenheitsdaten (also das was zum Beispiel gemäß EP 0 669 032 in den Gewichten des trainierten neuronalen Netzes abgespeichert wird) als lesbare und interpretier-/modifizierbare Fuzzy-Regeln zur Verfügung steht, sind diese in jeder Weise ergänz-, verifizier- und erweiterbar. Hinsichtlich der Eingangs- und Ausgangsdaten können die "neuronal" erzeugten Fuzzy-Regeln die gleichen Größen verwenden wie die Expertenregeln.

Die „neuronal“ erzeugten Fuzzy-Regeln beruhen vorzugsweise auf einer Analyse vorausgegangener Transaktionen hinsichtlich solcher Faktoren wie dem durchschnittlichen Betrag der Transaktion, dem Anteil von Barauszahlungen, dem Anteil von Auslandseinsätzen, von Reisekostennutzungen, dem früheren Auftreten von Verdachtsfällen usw. und hinsichtlich „dynamischer“ Kriterien wie etwa der aktuellen Ausschöpfung des Limits der betroffenen Kreditkarte. Das Ergebnis dieser Analyse wird

auch als „Zeitreihe“ bezeichnet. Dieses Regelsystem ermittelt so für jede Transaktion ein dynamisches Risiko in Form eines „Bonus“ bzw. „Malus“.

Die Erfindung gestattet so die Verschmelzung statistischer Modelle mit Expertenwissen. Statt, wie beim Stand der Technik, für jeden Vorgang einfach eine Betrugswahrscheinlichkeit auszurechnen, wird das für jede Transaktionsart definierte Limit gleitend mit dem dynamischen Risiko („Bonus“ oder „Malus“) der spezifischen aktuellen Transaktion zu einem (gleitenden) Transaktionslimit kombiniert.

Dies ermöglicht unterschiedliche, differenzierte Behandlungen „auffälliger“ Transaktionen, z.B. die sofortige Sperre oder statt dessen die Verweisung zur individuellen Überprüfung, z.B. durch einen Sachbearbeiter.

Im Stand der Technik wird eine Transaktion, die oberhalb der berechneten Risikoschwelle liegt, normalerweise gesperrt; der Stand der Technik kennt grundsätzlich nur Freigabe oder Sperre als Ergebnis der Überprüfung. Die Erfindung ermöglicht statt dessen abgestufte Reaktionen; beispielsweise kann ein Verdachtsfall generiert werden (und damit in die „Zeitreihe“ für diese Kreditkarte eingehen, die für zukünftige Transaktionen herangezogen wird), obwohl die aktuelle Transaktion autorisiert wird. Bei stärkerem Verdacht würde eine Nachprüfung (referral) der aktuellen Transaktion (vor deren eventuellen Freigabe) ausgelöst; bei noch stärkerem Verdacht würde die Transaktion verweigert (decline).

Wesentliche Unterschiede zum Stand der Technik ergeben sich auch hinsichtlich der Modellbildung, also der Generierung und Erkennung von Mißbrauchsmustern (Fraudmustern).

Der Stand der Technik basiert auf „passiver Datengewinnung“. Mit anderen Worten, ausschließlich bereits vorhandene Vergangenheitsdaten werden zur Modellbildung herangezogen. Das bedeutet, um im Modell überhaupt ein Fraudmuster erkennen zu

können, muß (a) bereits genug Zeit verstrichen sein, damit die Fraudmeldungen bereits zurückgekommen sind (meist erst, nachdem die Kunden ihren Auszug gelesen haben), (b) müssen genug Fälle für ein sicheres Training vorhanden sein (nur so funktioniert ein neuronales Netz / es gibt Fraudfälle, die sehr selten sind, aber einen hohen Einzelschaden ausmachen, die sind so nur sehr schwer im Modell zu erfassen, © erst nach einem aufwendigen manuellen Retraining ist eine Immunisierung des Autorisierungsbetriebes überhaupt möglich.

Hingegen ist die Datengewinnung erfindungsgemäß „aktiv“. Tauchen die ersten Verdachtsmomente eines neuen Fraudmusters auf, so werden Regeln definiert, die sofort eine Nachrecherche genau dieser Fälle durch aktive Kontaktierung der Kunden auslösen. So stehen im Idealfall innerhalb weniger Stunden viele gesicherte Daten darüber zur Verfügung, ob hier tatsächlich ein neues Fraudmuster aufgetaucht ist, und wie es sich von anderen Mustern abgrenzt. Diese Analyse läßt sich (egal mit welchem Verfahren) nämlich erst durchführen, wenn genug gesicherte Daten vorhanden sind.

Die Methodik der Modell-Erstellung im Stand der Technik führt dazu, daß die Erfahrung menschlicher Analysten zu wenig genutzt werden kann und Erwartungen über zukünftige Fraudmuster nicht Eingang finden können. Im Stand der Technik bildet das neuronale Netz praktisch eine „black box“ festgelegter, starrer Kriterien, die nur noch „automatisch“, also als Ergebnis wiederum vorher festgelegter Algorithmen, hinsichtlich der „Gewichte“ modifiziert werden. Soweit überhaupt Expertenregeln zusammen mit neuronalen Netzen eingesetzt werden, laufen neuronales Netz und Expertenregeln unabhängig nebeneinander. Durch den NeuroFuzzy-Ansatz ist das mit Daten trainierte prädiktive Modell keine black box mehr, sondern wird in Form von Fuzzy-Regeln erzeugt. Diese sind direkt von Experten interpretierbar und modifizierbar.

Die erfindungsgemäßen gleitenden Transaktionslimits erlauben eine wirkungsvolle Kombination von „hard facts“ und „soft facts“. Dies ermöglicht eine Modellierung der

„soft“ und „hard“ facts in konsistenter und kooperativer Weise. Bei dem „black-box“-Ansatz im Stand der Technik ist das nicht wichtig, denn dort findet keine wissensbasierte Modellierung statt. Bei der Erfindung, die es ermöglicht und vorzugsweise auch vorsieht, daß automatische Modellbildung und menschliche Expertise im laufenden Betrieb kombiniert werden, ist dies sehr relevant.

Im folgenden wird die Erfindung an einem Ausführungsbeispiel näher erläutert, welches gegenwärtig besonders bevorzugte Ausgestaltungen des erfindungsgemäßen Grundprinzips umfaßt.

Das Ausführungsbeispiel betrifft ein Autorisierungssystem für Kreditkarten-Transaktionen und damit eine Grundkonstellation ähnlich der im eingangs behandelten Stand der Technik. Aus einem vorhandenen Netzwerk, das Nutzungsstellen für die im System benutzbaren Kreditkarten umfaßt, kommen Autorisierungsanfragen, die in Echtzeit bearbeitet und beantwortet werden müssen.

Die Bearbeitung der Autorisierungsanfragen erfolgt im erfindungsgemäß ausgestalteten Autorisierungssystem, das schematisch in den Figuren 1 bis 4 gezeigt ist.

Das System umfaßt im Ausführungsbeispiel mehrere Rechner, kann aber natürlich auch auf einem Zentralrechner oder mittels eines Rechner-Netzwerks realisiert werden.

Im Beispiel umfaßt das System einen „Tandem“-Rechner mit einer Datenbank A, einen „SGI“-Server (SQL-Server) mit einer Datenbank B und ein „Hostsystem“ mit einer Datenbank C.

Auf dem Tandem-Rechner ist eine Software implementiert, die für Datenübergaben, Data Preprocessing (Kriterien-Ableitung), Zeitreihenberechnungen und -aktualisierungen etc. dient, wie später noch deutlich werden wird. Weiterhin ist auf dem Tandem-Rechner die

erfindungsgemäße Entscheidungslogik implementiert, die Fuzzy-Expertenregeln und Neuro-Fuzzy-Modelle umfaßt und die Entscheidung über die Autorisierungsanfragen trifft. Die auf dem Tandem-Rechner implementierte Software wird im folgenden zusammenfassend als „NeuroFuzzy Inferenzmaschine“ (NFI) bezeichnet.

Der SGI-Server dient, gegebenenfalls zusammen mit einer entsprechenden Zahl von PC-Clients, insbesondere zur Implementierung der Software für den „Investigation Workflow“ (IW) für die Nachbearbeitung von Verdachtsfällen, und für das „Online Data Mining Module“ (ODMM), wie später noch erläutert werden wird.

Das Hostsystem enthält und erhält die wesentlichen historischen wie aktuellen Daten zu Zahlungsmittel und Nutzer, die für die Bearbeitung der Autorisierungsanfragen benötigt werden.

Figur 1 zeigt den grundsätzlichen Informationsaustausch wie folgt:

Das Autorisierungssystem erlangt Daten (1) für ein Cardholder File aus der Datenbank [C] des Hostsystems. Bei einer Änderung der Daten des Cardholder Files werden nur die für die Autorisierung relevanten Daten einer Kartenummer auf das Autorisierungssystem überspielt. Ereignisse wie Kartensperrungen mit einer hohen Priorität werden sofort übertragen, andere mit einer kleineren Priorität erst wesentlich später. Der Datentransfer (Update) erfolgt stündlich.

Der SGI-Server erhält (2) über das bestehende Netzwerk vom Tandem-Autorisierungsrechner die Autorisierungsanfragen, versehen mit der von NFI ausgelösten Aktion (diese besteht aus: Fallwichtigkeit, Fallklasse, Fallschwelle, Referralentscheidung, Risiko-Score, Limit und Action Code) sowie die aktuelle Zeitreiheninformation. (Die hierfür erforderlichen Echtzeitanforderungen liegen im Bereich von Minuten. Die

Gesamtinformation zu einer Autorisierungsanfrage wird von der NFI zu einer Nachricht komprimiert, die dann an den SGI-Server übertragen wird.)

Weiter erhält der SGI-Server vom Hostsystem alle Postinginformationen, Mißbrauchsinformationen und gegebenenfalls Karteninhaberstammdaten, die nicht aus der Cardholder File extrahiert werden können (3). Die Datenbank des SGI-Servers [B] speichert diese Daten je nach Speicherausbau so lange wie erforderlich. Der SGI-Server beherbergt die Serverkomponente sei es des Supervisory Workflow (ODMM) als auch des Investigation Workflow (IW).

Figur 2 zeigt den Datenfluß bei vermuteten bzw. erkannten Mißbrauchsfällen.

Der Investigation Workflow (IW) (6) dient der Bearbeitung der erkannten und vermuteten Fraudfälle, insbesondere durch Mitarbeiter (Call-Center).

Im Call-Center wird festgestellt, ob es sich bei den vermuteten Mißbrauchsfällen um tatsächliche Mißbrauchsfälle handelt. Es erfolgt eine entsprechende Mitteilung (7) an den SGI-Server.

Neben dieser ersten Hauptaufgabe erfüllt der SGI-Server noch eine weitere Hauptaufgabe:

Die Datenbank des SGI-Servers speichert die für das Entdecken neuer Fraudmuster erforderlichen Daten und bereitet diese für eine Analyse durch das Online Data Mining Modul (ODMM) auf. Hierfür werden die mißbrauchsrelevanten Daten in der Datenbank [B] zwischengespeichert. Im Fraud Supervisory Center werden dann mittels dieser Informationen (4) neue Fraudregeln definiert und die vorhandenen Fraudregeln werden kontinuierlich auf ihre Wirksamkeit hin überprüft.

Die entsprechend modifizierten Fraudregeln in Form einer Datei werden vom Fraud Supervisory Center auf den Autorisierungsrechner übertragen (5). Hierzu wird vom PC aus die Datei auf den SGI-Server gebracht. Auf dem SGI-Server wird ein automatischer Job installiert, der erkennt, wenn der Timestamp der Datei sich geändert hat, und in diesem Falle einen Austausch der Datei auf der Tandem vornimmt, als auch der NFI mitteilt, daß es diese Datei neu einlesen muß.

Es ergeben sich somit insgesamt zwei Workflows (Figur 4):

1. Der Supervisory Workflow ODMM paßt die Entscheidungsstrategie des Präventionssystems kontinuierlich an die sich ändernden Mißbrauchsmuster an.
2. Der Investigation Workflow IW kontrolliert die Entscheidungen des Präventionssystems durch Einzelbearbeitung der gemeldeten und vermuteten Mißbrauchsfälle.

Beide Workflows sind indirekt über die (mittlere) operative EDV-Ebene verbunden. Wird im Supervisory Workflow die Entscheidungsstrategie modifiziert, so werden vom Präventionssystem andere Referrals generiert, die im Investigation Workflow nachrecherchiert werden.

Nicht vom Präventionssystem rechtzeitig erkannter Mißbrauch sowie fälschlicher Mißbrauchsverdacht wird vom Investigation Workflow verifiziert und in der Datenbank des SGI-Servers abgelegt. Hierauf greift das Online Data Mining Modul (ODMM) zu und schlägt den Fraudexperten im Fraud Supervisory Center entsprechende Modifikationen der Entscheidungsstrategie vor.

Die gesamte Berechnung, also der Fluß der Fuzzy-Inferenz durch das Regelwerk, sowie die gesamte Profilbildung und -initialisierung, wird von der NFI selbst übernommen; es ist keine externe Steuerung erforderlich. Die Schnittstelle enthält weitere Funktionen zur

Initialisierung und Konfiguration der Entscheidungslogik (diese Funktionen müssen einmal beim Laden des Präventionsmoduls aufgerufen werden), die aber nicht pro Autorisierungsanfrage aufgerufen werden müssen.

Die SQL-Datenbank des Autorisierungsrechners (Cardholder File) wird um ein Feld "Zeitreihe" ergänzt. Dieses Feld speichert die letzten Autorisierungsanfragen zu dieser Kartennummer (Nutzungsprofil) in komprimierter Form ab. Wenn eine Autorisierungsanfrage in das System kommt, wird der komplette Datensatz der Karte aus der Datenbank geladen. Hier muß nun zusätzlich noch das Binärobjekt "Zeitreihe" aus der Datenbank geladen und dem NFI zugeführt werden. Das Binärobjekt Kartennutzungsprofil wird in einer stark komprimierten Form erzeugt, so daß es in Form eines String in der SQL-Datenbank effizient für den Echtzeitzugriff gespeichert werden kann. Zusätzliche Rechenzeit durch das Auslesen und Wiedereinspeichern des Kartenprofils bei jeder Autorisierungsanfrage wird keinen spürbaren Rechenaufwand bedingen, da der Datensatz einer Karte sowieso bei jeder Autorisierungsanfrage ausgelesen wird. Nach der Entscheidung aktualisiert das NFI die Zeitreihe um die jetzt gerade eingegangene Autorisierung. Genau wie die durch die Autorisierung aktualisierten Limits muß auch die aktualisierte Zeitreihe wieder in die Datenbank zurückgeschrieben werden.

Weiterhin wird die Cardholder File ergänzt um zwei Datumsfelder, je eines für "kein Referral bis" (Dieses Feld wird bei einem positiv beantworteten Referral gesetzt, um sicherzustellen, daß nicht sofort nach einer positiven ID des Karteninhabers dieser bei der nächsten Transaktion direkt wieder einen Referral erhält) und eines für "Kurzreferral bis" (bei akutem Verdacht wird dieses Datum gesetzt, um bis zu diesem Datum bei jeder Autorisierungsanfrage einen Referral zwangsweise zu erzeugen.). Diese Felder werden über das Autorisierungssystem gesetzt oder zurückgesetzt. Die Daten werden vom Autorisierungssystem an die NFI übergeben, die NFI wertet die Daten aus und entscheidet, ob ein Referral oder Decline, und gegebenenfalls ein Fall generiert werden soll. Da die NFI gegebenenfalls auch mandantenabhängige Regeln enthält, muß die NFI den



Mandanten aus der Kartennummer erkennen. (Mandant ist z.B. der Kunde der Processingfirma, für welchen das Fraudprocessing durchgeführt wird)

Die Entwicklungskomponente ist Bestandteil des Supervisory Workflow und eine grafische Entwicklungs- und Analysesoftware, die auf Windows/NT Workstations (Clients) installiert wird. Hierbei kann es sich um vorhandene Rechner handeln, der auch für andere Aufgaben genutzt wird, oder es kann ein eigener Rechner bereitgestellt werden.

Von der Entwicklungssoftware aus kann der Entwickler das Fuzzy-Entscheidungssystem der Tandem modifizieren. Hierbei wird in keinem Fall der laufende Autorisierungsprozeß gestoppt, gestört oder verlangsamt.

Werden neue Betrugsprofile bekannt, so erlaubt die Entwicklungskomponente, diese durch Modifikation bekannter und Definition neuer Regeln zu berücksichtigen. Dabei werden diese neuen Regeln und modifizierten Regeln in die NFI übertragen, wo sich die neuen Regeln augenblicklich auf das Autorisierungsverhalten auswirken.

Alle Autorisierungsanfragen werden von der Tandem über TCP/IP an den SGI-Server übergeben. Der SGI-Server legt für jede Autorisierungsanfrage einen neuen Record an und füllt diesen mit allen erforderlichen Information.

Liegt die Fallwichtigkeit einer Autorisierungsanfrage über der Fallschwelle, so legt der SGI-Server zusätzlich einen Fall an. Ein Fall besteht aus einem Eintrag in der Falltabelle und den hierzu gehörigen Untertabellen.

Zusammengefaßt:

Jede von der Tandem eingehende Message beschreibt eine Autorisierungsanfrage.

Für jede Autorisierungsanfrage wird ein Record angelegt.

Die Fallerzeugung ist von den Referrals unabhängig, d.h. es kann ein Fall erzeugt werden, ohne daß ein Referral erzeugt wurde und es kann ein Referral erzeugt werden ohne daß ein Fall erzeugt wird.

Diese Schnittstelle ist auf Seiten der SGI-Server erstellt. Die Erzeugung der entsprechenden Einträge in den Tabellen des SGI-Servers ebenfalls.

Zur Nachbearbeitung der möglichen Betrugsfälle und Referrals dient der Investigation Workflow. Hierbei wird für die Fallsortierung die von der NFI ermittelte Fallwichtigkeit zugrundegelegt. Ob oder ob nicht für diese Autorisierungsanfrage ein Referral generiert wurde, ist für die Generierung eines Falles unerheblich. Die Fallgenerierung arbeitet mit einer eigenen Entscheidungslogik, die auch Regeln abweichend von den Betrugsregeln enthalten kann. Hierdurch lassen sich Präventionsstrategien sozusagen "erstmal im Trockenen" ausprobieren. Damit können im Investigation Workflow auch solche Fälle nachverfolgt werden, bei denen der Verdacht nicht für eine Referralgenerierung ausgereicht hat.

#### Komprimierte Speicherung der Autorisierungshistorie ("Zeitreihe")

Die NFI arbeitet mit neuronalen Modellen, die auf der Analyse früherer Transaktionen beruhen.

Problem einer solchen Analyse ist, daß während der Bearbeitung einer Autorisierungsanfrage keine Abfrage und Analyse vergangener Transaktionen in Echtzeit möglich ist. Daher muß die NFI eine Kurzhistorie in einem Ringpuffer zwischenspeichern. (Ein Ringpuffer ist ein Speicher mit einer festen Anzahl von Plätzen, die hintereinander geschaltet sind. Jedes neu gespeicherte Objekt wird "vorne" in den Ringpuffer

hineingeschoben, was alle bereits im Ringpuffer befindlichen Objekte je eine Position weiterschiebt. Das Objekt auf dem letzten Platz fällt dabei völlig aus dem Ringpuffer heraus.) Besonders wichtig ist hier, daß diese Zeitreihe so wenig Speicherplatz wie möglich erfordert (jedes Byte pro Karte ergibt einen Nettospeicherplatzbedarf von ungefähr 7 Megabyte in der Datenbank des Autorisierungsrechners), und so schnell und effizient wie möglich gelesen und geschrieben werden kann.

Aus diesem Grunde basiert die Zeitreihenbildung auf einem Algorithmus, der diesen Ringpuffer so erzeugt und aktualisiert, daß dieser effizient zu speichern und zu berechnen ist. Zur Speicherung wird eine komprimierte Speicherung im umgewandelten Ganzzahlformat verwendet.

Die Zeitreiheninformation stellt dabei z.B. eine verdichtete Historie der letzten 15 Autorisierungsanfragen dar, die eine Berechnung von dynamischen Kriterien (Ausschöpfung, Panik, Tankstellennutzung,...) ermöglicht. Die Zeitreiheninformation erlaubt zudem die Ermittlung von aggregierten Größen wie: Durchschnittliche Einkaufshöhe, Anteil Cashing, Anteil Ausland, Anteil Reisekostennutzung, wann wurde zum letzten Mal ein Referral ausgesprochen und wann wurde zum letzten Mal ein Referral beantwortet.

Da die Zeitreiheninformation 15 mal (für jede Autorisierungsanfrage im Ringpuffer) abgespeichert werden muß, ist hier eine Komprimierung der Information besonders wichtig.

Da in der Datenbank das Profil als Binärobjekt (Stringformat) abgespeichert wird, können die einzelnen Teilinformationen jeder Transaktion im Ringpuffer als Ganzzahlen beliebiger Bitlänge codiert werden. Es wurde allerdings eine sinnvolle Aufteilung einzelner Bitlängen auf die Bytes des Stringformats gewählt, damit die Berechnung und Aktualisierung der Profile nicht zu rechenaufwendig wird. Hierdurch ist nicht immer "auf

Bit genau" die kürzestmögliche Speicherform gewählt, sondern es ergibt sich ein Kompromiß aus Speicherplatzbedarfminimierung und Rechenperformancemaximierung.

Zu den gespeicherten Feldern im einzelnen:

- Datum

Die Abspeicherung des Datums im Minutenformat ermöglicht das einfache Berechnen von Zeitdifferenzen im Ganzzahlarithmetik einer 16-bit Zahl (mit 16-Bit Minutenauflösung lassen sich maximal 45 Tage darstellen, was für die Berechnung von Zeitdifferenzen im Profil ausreicht).

Die bei Subtraktionen solcher Minutenwerte resultierenden 16-Bit Werte für die Zeitdifferenzen werden direkt ohne rechenaufwendige Umskalierungen als Eingangsgrößen der NFI verwendet.

Mit der maximalen Speicherlänge des Minutendatums nach Stichtag von 24 Bit muß allerdings ein Reset der Profilinformatoren alle 31 Jahre erfolgen.

Ist dieser Eintrag "Datum" gleich "0", so bedeutet das, daß dieser Eintrag im Ringpuffer noch nicht verwendet ist.

- Betrag

Muß durch 10 dividiert werden, um den Euro-Betrag zu ergeben. Hierdurch ergibt sich eine optimierte Ausschöpfung des 20 bit Zahlenbereiches. Betragsabweichungen unter Euro 0,10 sind für die Mißbrauchsprävention unerheblich, und der maximale darstellbare Betrag von über Euro 100.000,00 ist auch ausreichend. Angefragte Werte über Euro 100.000,00 werden auf Euro 100.000,00 im Ringpuffer abgeschnitten.

- MCC

Enthält den Branchencodes des Vertragspartners, der die Autorisierung angefragt hat.

ICA

Beschreibt alle Issues anhand ihrer ICA-Nummern.

Country Code

Für die Zeitreihenbetrachtungen reicht der Country Code zur Herkunftsbestimmung aus. Dieser ist maximal dreistellig, daher reichen 10 bit zur Darstellung aus (nach MC Quick Reference Booklet, Oktober 97).

- POS

Nimmt die 5 möglichen POS Entry Modes auf. Zwar würden 3 bit ausreichen, um die 5 möglichen POS Entry Modes darzustellen, doch bietet die Darstellung in 4 bit rechnerische Vorteile.

- Status

Status beschreibt beispielsweise, ob das Verfallsdatum falsch war, oder ob ein CVC Problem aufgetreten ist, etc.. (Auf der Magnetkarte ist die Kartennummer um einen dreistelligen Code (CVC-1) erweitert. Dieser dreistellige Code ist nicht errechenbar. Damit ist über diese Prüfung eine recht gute Identifikation einer echten Karte möglich.)

Hierdurch ist gewährleistet, daß auch nichtautorisierte Anfragen in dem Profil berücksichtigt werden können.

### Fraud Supervisory Workflow

Der Fraud Supervisory Workflow umfaßt alle Werkzeuge, die verwendet werden, um die Entscheidungslogik zu kontrollieren und zu warten. Im einzelnen sind dies die Module:

#### - Online Data Mining Modul

Zur systematischen Erkennung neuer Mißbrauchsmuster, sowie zur kontinuierlichen Prüfung der Treffsicherheit aktuell definierter Entscheidungsregeln.

#### - Entscheidungslogik

In diesem Modul werden die Entscheidungskomponenten entwickelt, überwacht und gesteuert.

#### - Analyse-NFI

Die Analyse-NFI dient dem Test neuer Entscheidungslogiken an Vergangenheitsszenarien.

### Online Data Mining Modul (ODMM)

Das Online Data Mining Modul besteht sowohl aus einer Serverkomponente auf dem SQL-Server als auch aus einer Clientkomponente auf PC. Die Clientkomponente arbeitet mit dem Server über Pass-Through Queries und verknüpfte Tabellen zusammen.

Das ODMM arbeitet mit den Tabellen, in denen die für die Analysen erforderlichen Autorisierungsanfragen und Fälle abgelegt sind.

Der ODMM Client erhält folgende Informationen zu jeder Transaktion:

- Kartenummer (Zusammen mit Datum und Zeit der Transaktion dient diese Information der eindeutigen Zuordnung jeder Transaktion (Schlüssel). Da zu einer Transaktion mehrere Ereignisse (zum Beispiel mehrere Autorisierungsanfragen, Mißbrauchsmeldungen, beantwortete Referrals, etc.) gehören können, die zu unterschiedlichen Zeiten stattfinden können, wird hier immer das früheste Datum eingesetzt. Dies entspricht der Logik, daß die zu dieser Transaktion gehörenden Ereignisse sich alle auf den ersten Zahlungswunsch beziehen, der im System bekannt geworden ist.
- Datum und Zeit der Transaktion
- Betrag in Euro
- Typ der Transaktion (autorisierte oder nichtautorisierte Transaktion; bei nicht-autorisierten Transaktionen liegt beispielsweise keine Autorisierungsanfrage vor, jedoch kann beispielsweise ein Posting und eine Mißbrauchsmeldung vorliegen)
- Mißbrauch (ist Mißbrauch aufgetreten?)
- Referral (ist ein Referral generiert worden, wenn ja, wie beantwortet)
- Informationen aus der Autorisierungsanfrage oder dem Posting (Branchencode, Country Code Herkunft, POS Entry)
- Zufallszahl (Auswahl einer Stichprobenmenge)

Die Tabellen, die diese Informationen liefern, werden von den ODMM Clients über Pass Through Queries abgefragt.

Der Server ordnet im Nachhinein eintreffende Mißbrauchsmeldungen zu bereits in der Tabelle TRX eingetragenen Transaktionen zu. Ebenfalls werden die Ergebnisse für die statistische Komponente aktualisiert.

#### - Rasterfahndung

Die Rasterfahndung läuft als Pass-Through Query auf dem Server und generiert eine Tabelle mit Regeln, die aktuell nicht aktiviert sind und von denen es sinnvoll wäre, sie aufzunehmen. Jeder Regel ist eine Mißbrauchssumme zugeordnet, die im Untersuchungszeitraum hätte verhindert werden können, wenn diese Regel aktiv gewesen wäre. Um diese Aussage zu verifizieren, enthält jede Regel auch das Verhältnis fälschlich zu gerechtfertigt abgelehnter Autorisierungsanfragen (F/P-Rate), die Anzahl gerechtfertigter und die Anzahl nicht gerechtfertigter Referrals, welche die Beurteilung zur Aufnahme oder Ablehnung der Regel ermöglichen. Es ist möglich, die Regeln vorweg durch Angabe eines bestimmten Mißbrauchsbetrags und F/P-Rate zu filtern. Bei kleineren Summen oder höheren F/P-Raten werden die gefundenen Regeln ausgeblendet. Auch die Gewichtung zwischen der Mißbrauchssumme und der F/P-Rate kann bei der Sortierung eingestellt werden. Damit kann bei jeder Rasterfahndung erneut festgelegt werden, wie bedeutend jede der beiden Größen für die Untersuchung sein soll.

#### - Regelloptimierung

Die negativ beantworteten Referrals, die keinen Mißbrauch bestätigen konnten, dienen der Empfehlung zur Deaktivierung von Regeln als Grundlage. Wird ein Referral negativ beantwortet, so wird der dazugehörige Datensatz nicht mehr als Mißbrauch, sondern als

gute Transaktion in die Analyse einfließen. Sollte sich dann herausstellen, daß die Regel nicht genug Mißbrauch verhindert hat und zu viele gute Transaktionen verhindert hat, so wird sie zur Deaktivierung vorgeschlagen. Auch in dieser Analyse kann die Gewichtung zwischen der Mißbrauchssumme und der F/P-Rate eingestellt werden. Damit kann auch hier bei jeder Rasterfahndung erneut festgelegt werden, wie bedeutend jede der beiden Größen für die Untersuchung sein soll.

### Entscheidungslogik

Der Zugriff auf die Entscheidungslogik erfolgt über den Fraud Supervisory Workflow:

Der Block "Fraud Supervisory Workflow" stellt die PC-Netzwerke im Stab-SI dar. Diese verwalten beliebig viele Entscheidungslogiken, sei es zur Archivierung als auch als Zwischenstände der Entwicklung. (Die eigentlichen Daten für die Entscheidungslogiken werden zentral auf dem SGI-Server gespeichert, so daß alle Fraud-Analysten hierauf Zugriff haben. Der Zugriff auf diese Entscheidungslogiken erfolgt durch die PC mit der "Fraud Supervisory Workflow" Software.) Jede der Entscheidungslogiken besteht aus den drei Komponenten Listen, Zeitreihe und Regeln. Durch Druck auf die jeweilige Taste öffnen sich die entsprechenden Editoren für die Komponenten.

Im Produktivbetrieb läuft immer die Entscheidungslogik "Betrieb". Durch Druck der Taste [übertragen] wird die aktuell im PC entwickelte Entscheidungslogik "Betrieb" auf die Tandem übertragen und aktiviert.

Auf dem SGI-Server laufen beide Entscheidungslogiken für die Szenarienanalyse. Durch Druck der Taste [übertragen] wird die aktuell im PC entwickelte Entscheidungslogik "Test" auf die SGI-Server übertragen und aktiviert.

### Vorgehensweise bei der Entwicklung

Die grundsätzliche Vorgehensweise bei der Entwicklung von Entscheidungslogiken ist die folgende. Auf dem Autorisierungsrechner läuft die Entscheidungslogik "Betrieb". Durch Drücken der Taste [übertragen] wird die Entscheidungslogik "Test" mit der Entscheidungslogik "Betrieb" überschrieben. (Hierbei handelt es sich nicht um ein physikalisches Überschreiben von der Tandem auf die SGI-Server. Die SGI-Server verfügen ebenfalls über eine Kopie der Entscheidungslogik, wodurch das Überschreiben direkt auf den SGI-Servern ausgeführt wird.)

Hierdurch kann nun die Entscheidungslogik "Test" auf dem PC modifiziert werden und mit Hilfe der Analyse-NFI erfolgt der Test von Modifikationen durch direkten Vergleich des "Test"-Systems mit dem "Betriebs"-System.

Sind die an der Entscheidungslogik "Test" durchgeführten Modifikationen erfolgreich, so wird durch Drücken der Taste [übertragen] die Entscheidungslogik "Test" mit der Entscheidungslogik "Betrieb" überschrieben. Nachdem die neue Entscheidungslogik in Betrieb gegangen ist, fängt die Vorgehensweise erneut an.

Jede neue Transaktion wird von der NFI-Maschine mit einer Fallwürdigkeitsbeurteilung versehen. Ein Hilfsmodul kennzeichnet eine Transaktion als Fall, wenn sie ein Fallkriterium erfüllt (MCC, ICA, CNT, POS, Betragsklasse, Fallwürdigkeit).

Wie weit die Historie der Transaktionen und Postings eines Vorgangs zurückgeht, kann wahlweise bestimmt werden. Als sinnvoll wird ein Zeitraum von 4-6 Wochen erachtet.

Gehört eine Transaktion zu einer Kategorie aller möglichen Fälle, so wird ein neuer Record in der Investigation Workflow eigenen Tabelle angelegt. Dieser Record enthält folgende Einzelinformationen:

- Kartennummer
- Transaktionsdaten (Datum/Uhrzeit, MCC, CNT, ICA, POS, Betrag,)
- Fallstatus (ist der Fall neu oder wurde er abgeschlossen)
- Fallwichtigkeit (die Fallwichtigkeit FW stellt den NFI-Score dar)
- Fallklasse (Die Fallklasse gibt an, warum eine Transaktion zu einem Nachbearbeitungsfall geworden ist bzw. zu welcher Kategorie die Transaktion gehört. Die Kennung beinhaltet folglich Angaben über MCC, ICA, CNT, POS, Betragsklasse, FW.)
- Benutzername
- Wiedervorlagedatum
- Close-Status (Der Close-Status eines Falls gibt Auskunft über das Ergebnis der Bearbeitung nach Schließen des Falls und kann folgende Information enthalten: "Kein Betrug" oder "kein Betrug geschätzt", "Betrugsbestätigung unmöglich" oder "Betrug" oder "Betrug geschätzt".)

Die Kartennummer ist das Bindeglied (Zeiger) zu den vergangenen Transaktionen mit derselben Kartennummer auf dem DBMS des SGI-Servers. Zusammen mit den Stammdaten der Kartennummer sind alle Daten für den Fraud Investigation Workflow vollständig.

#### Eingangsgrößen der NFI

Die NFI wird über ein Tokenprotokoll in den Ablauf der Autorisierung integriert. Hieraus entnimmt die NFI alle Eingangsgrößen sowie die Zeitreihe als Binärdatenobjekt (String).

Als Sonderform der Autorisierungen hat die NFI die Nachrichten über eine Referralsperre oder ein Referral\_bis zu interpretieren.

**Referral\_bis:** Der Parameter Referral \_bis (Kurzreferral) wird bei Mißbrauchsverdacht zur Verhinderung von Genehmigungen benutzt. Es wird manuell mittels einer Autorisierung aktiviert.

Die NFI speichert das Referral\_bis Datum im Kartenprofil ab und überprüft bei der Autorisierung, ob das Transaktionsdatum kleiner dem Referral\_bis Datum ist. Ist dies der Fall, wird immer ein Referral von der NFI generiert.

Das Referral\_bis Parameter wird zur Analyse und Rekonstruktion als Bestandteil des Transaktionsdatensatzes über die TCP/IP-Schnittstelle zum SGI-Rechner übertragen.

**Referralsperre:** Die Referralsperre wird dazu benutzt, nach einer positiven Identifikation oder nach Sichtung der vergangenen Transaktionen die weitere Auslösung von Referrals zu unterbinden. Die Referralsperre kann die Zustände "gültig" oder "nicht gültig" annehmen. Ist sie "gültig", so wird ein vorher eingestellter Parameter, der einen festen Offset vom aktuellen Transaktionsdatum (zum Beispiel Transaktionsdatum + 3 Tage) angibt, aktiviert. Die Referralsperre ist immer in Form des Datums gegeben, bis zu dem sie gehen soll. Es kann ja nur zum aktuellen Zeitpunkt bestimmt werden, ob die Sperre damit gültig ist oder nicht.

Die Referralsperre kann einerseits vom Investigation Workflow aus aktiviert werden. Andererseits kann die Referralsperre auch indirekt vom Genehmigungsservice ausgelöst werden, wenn nach einem Referral eine positive Identitäts-Überprüfung stattgefunden hat. Nach einer positiven IdentitätsÜberprüfung wird vom Genehmigungsdienst eine Transaktion ausgelöst, die in der NFI verarbeitet wird. Die NFI schreibt die aktuelle Referralsperre in die Cardholder File auf dem Autorisierungsrechner.

Der Fall, daß sowohl eine Referralsperre als auch das Referral\_bis Datum gültig ist, muß vermieden werden. Daher wird beim Setzen eines Wertes (zum Beispiel Referral\_bis) der jeweils andere gelöscht (zum Beispiel Referralsperre).

### Interne Ausgangsgrößen

Liegen alle Eingangsgrößen vor, die von der NFI verwendet werden, so erzeugt die NFI intern 6 Ausgangsgrößen:

1. Limit
2. RiskScore
3. Fallwichtigkeit
4. Fallschwelle
5. Fallbegründung
6. Decline

Hierbei stellt Limit direkt das transaktionsindividuelle Limit für die aktuelle Autorisierungsanfrage dar. Dieses transaktionsindividuelle Limit wird durch den RiskScore als Malus vermindert ("gleitendes Transaktionslimit").

Die NFI entscheidet nun durch einfachen Vergleich, ob ein Referral erzeugt werden soll oder nicht. Ein Referral wird immer dann erzeugt, wenn der zur Autorisierung angefragte Betrag über dem transaktionsindividuellen Limit liegt. Durch die Größen "Referralsperre" und "Referral\_bis" kann die Entscheidung der NFI modifiziert werden.

Die weiteren drei Größen stellen die Entscheidung der NFI bezüglich der Fallgenerierung dar. Die Fallwichtigkeit stellt dar, in zu welchem Grade die aktuelle Autorisierungsanfrage als Fall erzeugt werden soll. Liegt dieser Wert über der Fallschwelle, so wird für die Autorisierung ein Fall erzeugt. Zusätzlich wird als Begründung der Entscheidung, einen

Fall aus dieser Autorisierungsnachricht zu generieren, ein Text "Fallklasse" erzeugt, der die Verdachtsart mit Worten beschreibt. Diese Beschreibung wird von dem Mitarbeitern des Investigation Workflow genutzt, um eine gezielte Ermittlungsarbeit durchführen zu können.

Diese Ausgangsgrößen der NFI werden direkt mit der gesamten Information zu der

- Autorisierung an die Autorisierungsanfrage übertragen. Die bestehende Software zur Autorisierung bearbeitet diese Information dann weiter.

Nach der Berechnung der NFI übergibt die NFI an das System die aktualisierte Zeitreihe. Das System speichert diese in der Cardholder File, um sie bei der nächsten Autorisierungsanfrage dieser Kartenummer wieder an die NFI zu übergeben.

Die eigentlichen Entscheidungsregeln der NFI werden in einer Datei auf dem Autorisierungsrechner abgelegt. Diese Datei wird von dem Entwicklungswerkzeug auf dem PC erzeugt.

Im folgenden wird die Entscheidungslogik näher erläutert. Dabei werden folgende Abkürzungen verwendet:

Tabelle 1

AvailBal	Noch verfügbarer Betrag auf der Karte in Euro
Betrag	Betrag, der zur Autorisierung angefragt wird (in Euro)
BranchenCode	Einzelne Branchencodes

Branchenklasse	Klasse der Branche, zu der der VP gehört
CountryCode	Ländercode aus der Autorisierungsnachricht
CurrencyCode	Währungscode aus Autorisierungsnachricht
GAC	Action Code aus Listendefinition
ICA_BIN	Herkunft der Transaktion
Inanspruchnahme	Noch zu definieren!
Kartenalter	Alter der Karte in Tagen gemessen an der Zeit, die seit "gültig ab neu" vergangen ist
Kartenlimit	Limit der Karte in Euro
KI_Range	Zugehörigkeit der Kartenummer zu Ranges, die als Liste definiert sind
letzte Antwort	Wie lange ist der letzte beantwortete Referral/Callme her?
letzte GAA	Zeit, die seit der letzten GAA-Abhebung vergangen ist
letzter Referral	Wie lange ist der letzte Referral/Callme her?
Mandant	Identifikation des Mandanten
Merchant_ID	Merchant ID aus Listendefinition
Panikfaktor	ist noch zu definieren!
POS_Eingabe	Eingabeart der Autorisierungsanfrage
Terminal_ID	Terminal ID aus Listendefinition
Z01	Eingangsvariable des Zählers XXXX

Die folgende Abbildung zeigt die Struktur für dieses Fuzzysystem mit Eingangsinterfaces, Regelblöcken und Ausgangsinterfaces. Die Verbindungslinien symbolisieren hierbei den Datenfluß.

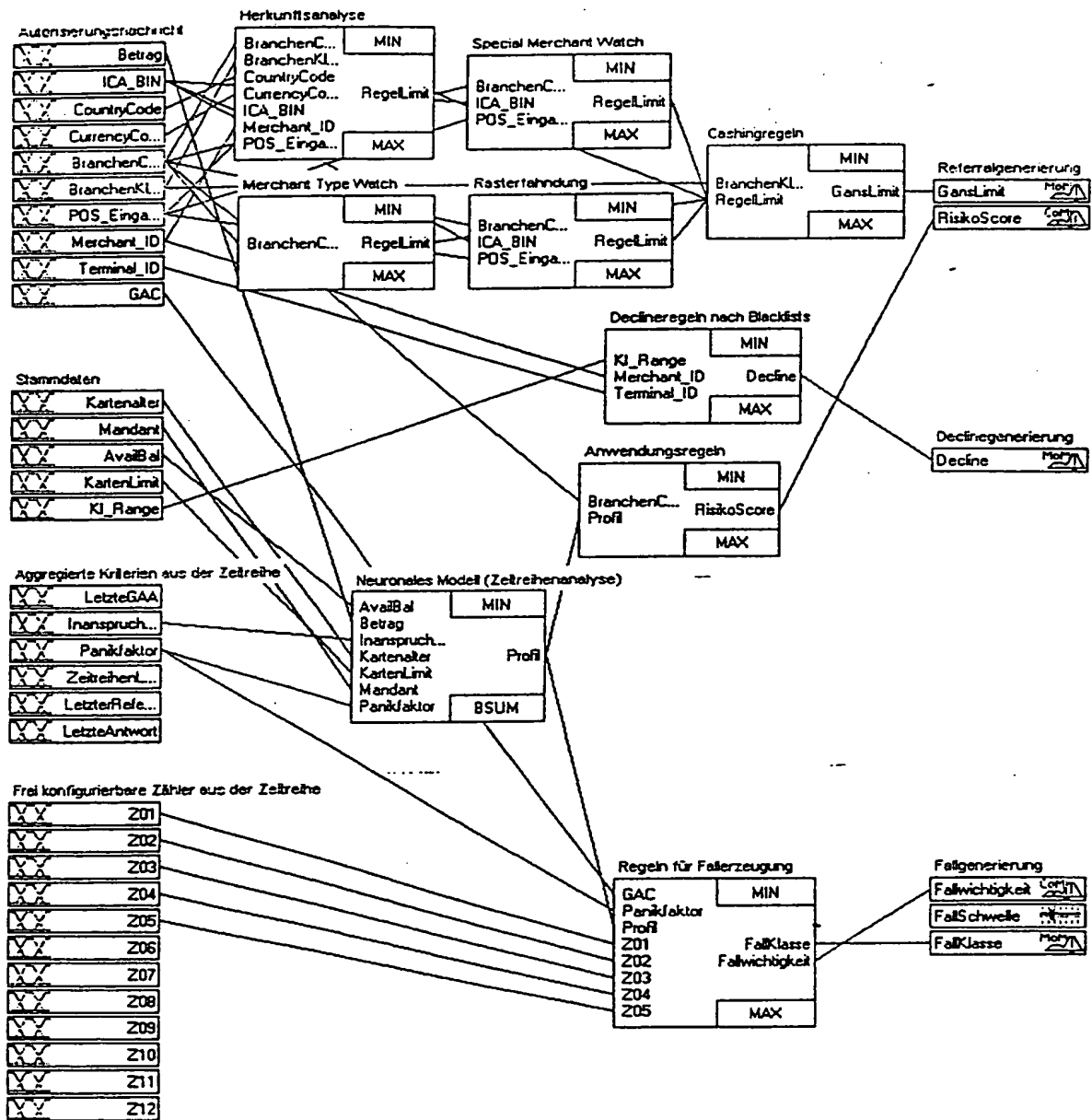


Abbildung 1: Struktur des Fuzzy Logic-Systems

Linguistische Variablen dienen in einem Fuzzysystem dazu, die Werte kontinuierlicher Größen durch sprachliche Begriffe zu beschreiben. Die möglichen Werte einer linguistischen Variablen sind keine Zahlen, sondern sprachliche Begriffe, auch Terme genannt.

Für alle Eingangs-, Ausgangs- und Zwischengrößen des Fuzzy-Systems werden linguistische Variablen definiert. Die Zugehörigkeitsfunktionen der Terme sind durch Stützstellen, die sogenannten Definitionspunkte, eindeutig festgelegt.

Die folgende Tabelle listet alle linguistischen Variablen zusammen mit den Termnamen auf.

Tabelle 2: Linguistische Variablen

AvailBal	niedrig, mittel, hoch
Betrag	niedrig, mittel, größer_1000, hoch
BranchenCode	FlugAllg, Kaufhaus, Pelze, Teppiche, Schallplatten, Nacht-lokale, Waffensprot, Juwelier, Foto, Leder, alle Banking, HotelAllg, alle5erMCC, Massage, AutoAllg, FunFreizeit
Branchenklasse	Hotel, Airlines, Auto, Buiz_serv, Car_rentals, Cashing, Clothing, contrctd_services, mail_order, misc_store, nicht5311, pers_services, retail, services, transportation, utilities, -cashing
CountryCode	Ägypten, Brasilien, Equador, Hongkong, Indonesien, Israel, Kolumbien, Malaysia, Marokko, Mexiko, Singapur, Thailand, Türkei, Venezuela, Kanada
CurrencyCode	f_franc, drachme, forinth, gulden, i_lira, peseta, pfund
GAC	bad_cvc
ICA_BIN	Visa_quer, mexiko_spezial, -mexiko_spezial
Inanspruchnahme	niedrig, mittel, hoch
Kartenalter	sehr_neu, neu, alt
Kartenlimit	niedrig, mittel, hoch
KI_Range	kein_range, fraud_nz, alle_anderen
letzte Antwort	gerade_erst, v_lang_her
letzte GAA	gerade_erst, mittel, lang_her

letzter Referral	gerade_erst, v_lang_her
Mandant	kein_mandant, gzs, airplus
Merchant_ID	wempe
Panikfaktor	niedrig, mittel, hoch
POS_Eingabe	unbekannt, unbek_o_manuell, manuell, gelesen, electr_ commerce, gelesen_geprüft
Terminal_ID	krimin_figaro
Z01	mehr_als_vier
Z02	mehr_als_vier
Z03	mehr_als_vier
Z04	mehr_als_vier
Z05	mehr_als_vier
Z06	mehr_als_vier
Z07	mehr_als_vier
Z08	mehr_als_vier
Z09	mehr_als_vier
Z10	mehr_als_vier
Z11	mehr_als_vier
Z12	mehr_als_vier
Zeitreihenlänge	hoch
Decline	kein_decline, decline

Fallklasse	counterfeit, hongkong, cvc_queue, ungarn, watchlist, juweliere
Fallwichtigkeit	unverdächtig, mittel, verdächtig
Limit	_0,_100,_250,_500,_1000,_2500,_7500
RisikoScore	unverdächtig, mittel, verdächtig
Profil	unverdächtig, riskant
Regel-Limit	_0,_100,_250,_500,_1000,_2500,_7500

Die Eigenschaften der Basisvariablen sind in der folgenden Tabelle aufgelistet.

Tabelle 3: Basisvariablen

Variablenname	Min	Max	Default	Einheit
AvailBal	0	20000	0	Euro
Betrag	0	20000	0	Euro
BranchenCode	0	9999	0	MCC
Branchenklasse	0	32	0	Codewert_Liste
CountryCode	0	999	0	CC_Schlüssel
CurrencyCode	0	999	0	CC_Schlüssel
GAC	0	32	0	Codewert_Liste
ICA_BIN	0	32	0	Codewert_Liste
Inanspruch-	0	100	0	Prozent

nahme				
Kartenalter	0	100	0	Tage
Kartenlimit	0	20000	0	Euro
KI_Range	0	32	0	Codewert_Liste
letzte Antwort	0	45	45	Tage
letzte GAA	0	45	0	Tage
letzter Referral	0	45	45	Tage
Mandant	0	32	0	Codewert_Liste
Merchant_ID	0	32	0	Codewert_Liste
Panikfaktor	0	100	0	Prozent
POS_Eingabe	0	32	0	POS_Entry_ Mode
Terminal_ID	0	32	0	Codewert_Liste
Z01	0	32	0	Anzahl
Z02	0	32	0	Anzahl
Z03	0	32	0	Anzahl
Z04	0	32	0	Anzahl
Z05	0	32	0	Anzahl
Z06	0	32	0	Anzahl
Z07	0	32	0	Anzahl
Z08	0	32	0	Anzahl

Z09	0	32	0	Anzahl
Z10	0	32	0	Anzahl
Z11	0	32	0	Anzahl
Z12	0	32	0	Anzahl
Zeitreihenlänge	0	32	0	AutoriAnfragen
Decline	0	1	0	-
Fallklasse	0	32	0	Codewert_Liste
Fallschwelle	0	1000	750	Schwelle
Fallwichtigkeit	0	1000	0	Promille
Limit	0	30000	0	Euro
RisikoScore	0	1000	0	Promille

Der Defaultwert wird von der Ausgangsvariablen angenommen, wenn für diese Variable keine Regel feuert. Für die Defuzzifizierung können unterschiedliche Methoden eingesetzt werden, die entweder das "plausibelste Resultat" oder den "besten" Kompromiß liefern.

Zu den kompromißbildenden Verfahren gehören:

CoM (Center of Maximum)

CoA (Center of Area)

CoA BSUM, eine Variante für effiziente VLSI-Implementierungen

Das "plausibelste Resultat" liefern:

MoM (Mean of Maximum)

MoM BSUM, eine Variante für effiziente VLSI-Implementierungen

Die folgende Tabelle listet alle mit einem Interface verknüpften Variablen auf, sowie die entsprechende Fuzzifizierungs- bzw. Defuzzifizierungsmethode.

Tabelle 4: Interfaces

Variablenname	Typ	Fuzzifizierung/ Defuzzifizierung
AvailBal	Eingang	Berechne MBF
Betrag	Eingang	Berechne MBF
BranchenCode	Eingang	Berechne MBF
Branchenklasse	Eingang	Berechne MBF
CountryCode	Eingang	Berechne MBF
CurrencyCode	Eingang	Berechne MBF
GAC	Eingang	Berechne MBF
ICA_BIN	Eingang	Berechne MBF
Inanspruchnahme	Eingang	Berechne MBF
Kartenalter	Eingang	Berechne MBF
Kartenlimit	Eingang	Berechne MBF
KI_Range	Eingang	Berechne MBF
letzte Antwort	Eingang	Berechne MBF
letzte GAA	Eingang	Berechne MBF

letzter Referral	Eingang	Berechne MBF
Mandant	Eingang	Berechne MBF
Merchant_ID	Eingang	Berechne MBF
Panikfaktor	Eingang	Berechne MBF
POS_Eingabe	Eingang	Berechne MBF
Terminal_ID	Eingang	Berechne MBF
Z01	Eingang	Berechne MBF
Z02	Eingang	Berechne MBF
Z03	Eingang	Berechne MBF
Z04	Eingang	Berechne MBF
Z05	Eingang	Berechne MBF
Z06	Eingang	Berechne MBF
Z07	Eingang	Berechne MBF
Z08	Eingang	Berechne MBF
Z09	Eingang	Berechne MBF
Z10	Eingang	Berechne MBF
Z11	Eingang	Berechne MBF
Z12	Eingang	Berechne MBF
Zeitreihenlänge	Eingang	Berechne MBF
Decline	Ausgang	MoM
Fallklasse	Ausgang	MoM

Fallschwelle	Ausgang	Vorgabe
Fallwichtigkeit	Ausgang	CoM
Limit	Ausgang	MoM
RisikoScore	Ausgang	CoM

### Regelblöcke

Das Verhalten des Reglers in den verschiedenen Prozeßsituationen wird durch die Regelblöcke festgelegt. Jeder einzelne Regelblock enthält Regeln für einen festen Satz von Eingangs- und Ausgangsvariablen.

Der "wenn"-Teil der Regeln beschreibt dabei die Situation, in der die Regel gelten soll, der "dann"-Teil die Reaktion hierauf. Durch den "Degree of Support" (DoS) kann hierbei den einzelnen Regeln ein unterschiedliches Gewicht gegeben werden.

Zur Auswertung der Regeln wird zuerst der "wenn"-Teil berechnet. Hierbei können verschiedene Verfahren eingesetzt werden, die durch den Operatortyp des Regelblocks festgelegt sind. Der Operator kann vom Typ MIN-MAX, MIN-AVG oder GAMMA sein. Das Verhalten des Operators wird zusätzlich durch eine Parametrisierung beeinflusst.

Beispielsweise:

MIN-MAX, mit dem Parameterwert 0	= Minimum-Operator (MIN).
MIN-MAX, mit dem Parameterwert 1	= Maximum-Operator (MAX).
GAMMA, mit dem Parameterwert 0	= Produkt-Operator (PROD).

Der Minimum-Operator ist die Verallgemeinerung des booleschen "und" und der Maximum-Operator ist die Verallgemeinerung des booleschen "oder".

Die Ergebnisse der einzelnen Regeln werden bei der anschließenden Fuzzy-Composition zu Gesamtschlußfolgerungen zusammengefaßt. Die BSUM-Methode betrachtet hierbei alle für einen Zustand feuernden Regeln, während die MAX-Methode nur dominante Regeln berücksichtigt.

## ANSPRÜCHE

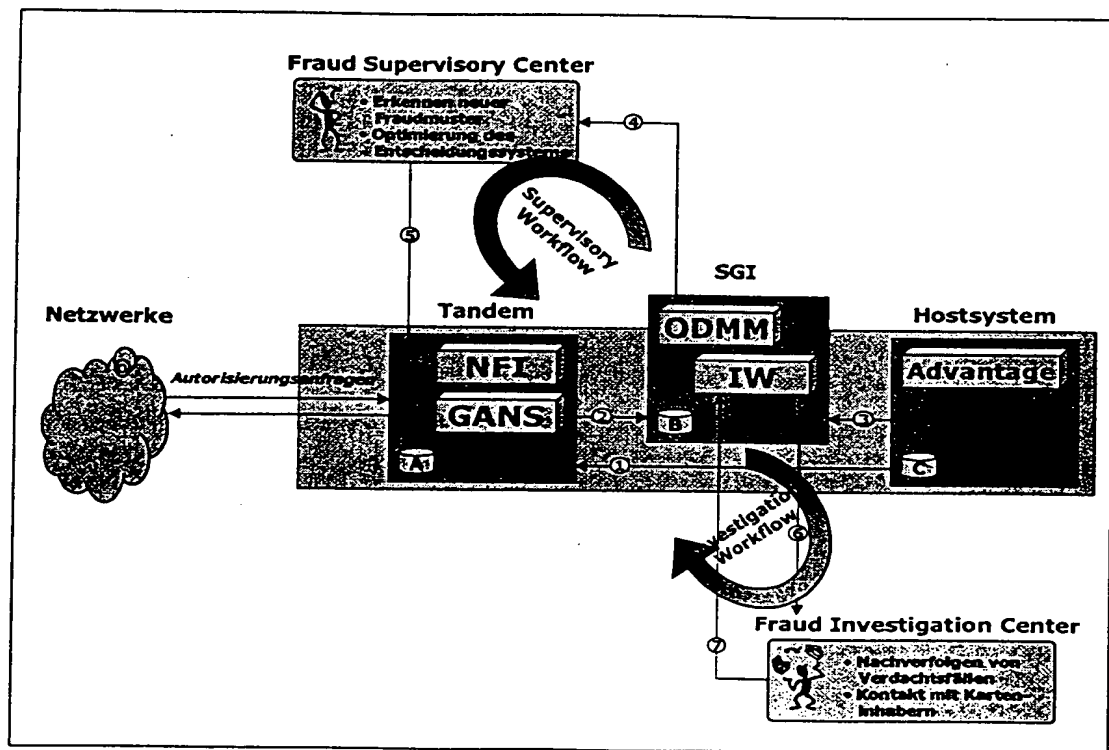
1. Auf einem Rechner realisiertes Verfahren zum Identifizieren und Ermitteln betrügerischer Transaktionsdaten in einem rechnergesteuerten Transaktionsverarbeitungssystem mit einem Vorhersagemodell zum Empfangen aktueller Transaktionsdaten, Verarbeiten der aktuellen Transaktionsdaten und Ausgeben wenigstens eines Ausgangswertes, der eine Wahrscheinlichkeit einer betrügerischen Transaktion wiedergibt, bei dem auf Grundlage gespeicherter Daten zu

- einer Zeitreihenanalyse früherer Transaktionen bezüglich des gleichen Zahlungsmittels bzw. Benutzers und
- Expertenregeln hinsichtlich bei betrügerischen Transaktionen statistisch signifikant gehäuft auftretenden Parametern, insbesondere bezüglich der Herkunft des Zahlungsmittels/Benutzers, der Branche und der Person des durch die Transaktion Begünstigten, sowie Höhe bzw. Wert der Transaktion, mittels des Vorhersagemodells die Bewertung hinsichtlich des Risikos erfolgt, daß die aktuelle Transaktion betrügerisch ist, und ein entsprechender Ausgangswert erzeugt wird,

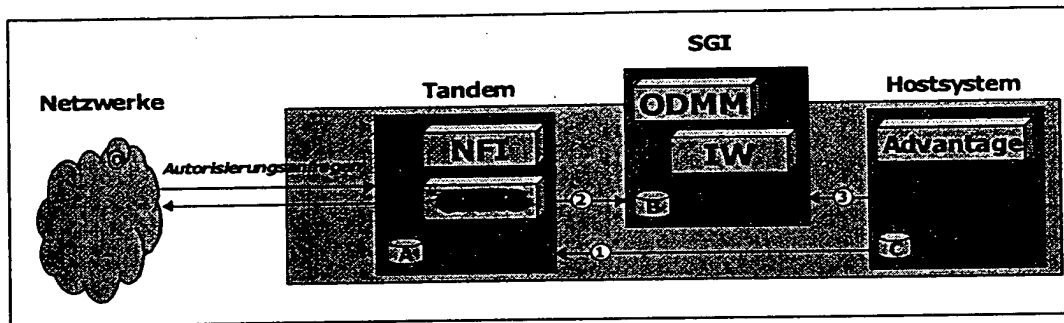
**dadurch gekennzeichnet, daß** das Prädiktionsmodell ein im wesentlichen auf den Expertenregeln basierendes, für die Art der Transaktion, spezifisches Limit mit einem im wesentlichen auf der Zeitreihenanalyse basierenden für die aktuelle Transaktion spezifischen Wert kombiniert, um den Ausgangswert zu erzeugen,

wobei die Kombination gleitend erfolgt, so daß je nach Stärke des Mißbrauchsverdachts verschiedene Ausgangswerte erzeugt werden können, die zur Auslösung unterschiedlicher Reaktionen auf der aktuellen Transaktionsanfrage benutzt werden können.

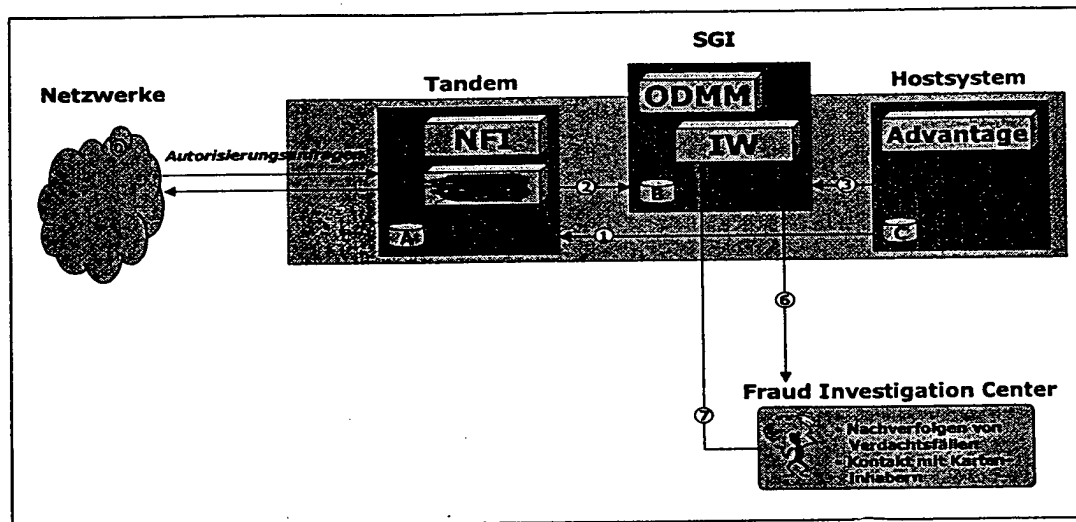
2. Verfahren nach Anspruch 1, bei dem die Zeitreihenanalyse in Form von Fuzzy-Logik-Regeln implementiert ist.



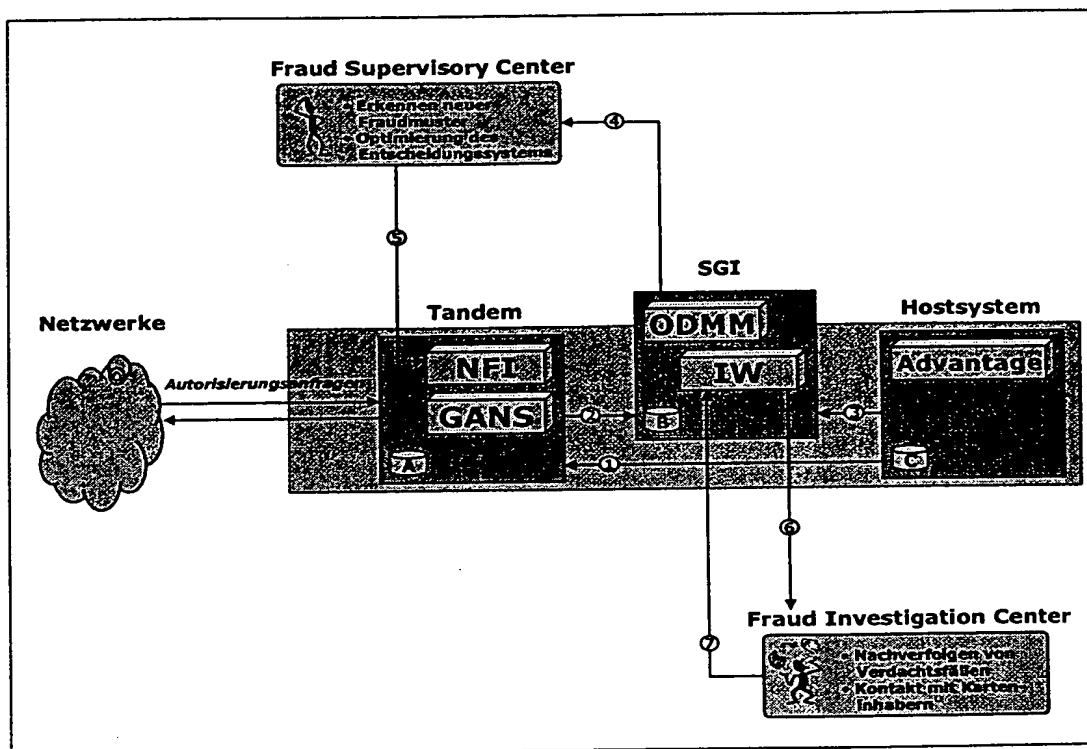
FIGUR 4



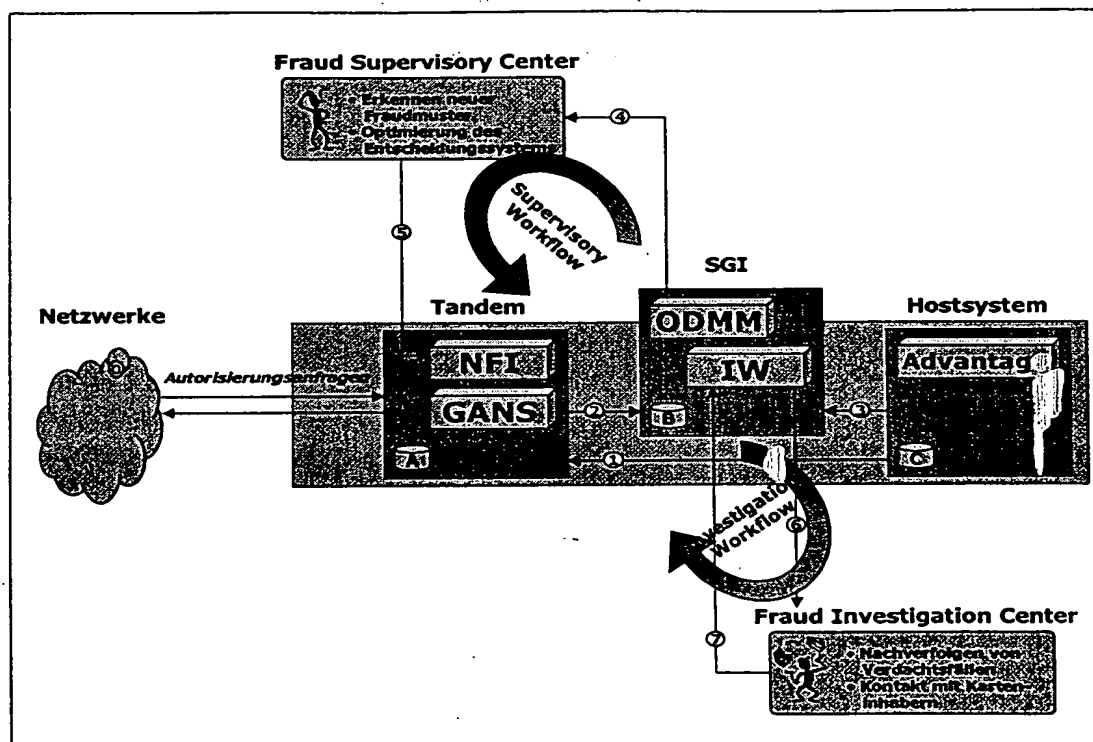
FIGUR 1



FIGUR 2



FIGUR 3



FIGUR 4

**THIS PAGE BLANK (USPTO)**